

APR 17 2007

U.S. Ser. No. 09/863,139
Attorney Docket No. 010055B1**REMARKS**

Claims 1-32 are pending in the present application. Claims 1-16 have been allowed, claim 17 was rejected, and claims 18-32 have been newly added. Applicant believes that the present application is in condition for allowance, and respectfully requests reconsideration of the rejection in light of the remarks set forth below.

I. REJECTION UNDER 35 U.S.C. §102

The Office Action rejected claim 17 under 35 U.S.C. §102(e) as being allegedly anticipated by U.S. Patent No. 6,225,888 issued to Juopperi. The rejection is respectfully traversed in its entirety.

To anticipate a claim under 35 U.S.C. § 102(e), the reference must teach every element of the claim and "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." (see MPEP §2131).

The Office Action states that Juopperi teaches every element of claim 17. Applicant respectfully disagrees with the characterization of Juopperi for the following reasons.

Juopperi discusses a method for a mobile station to request a communication channel from a base station. Juopperi teaches using authentication between the mobile station and base station to prevent an unauthorized third party from posing as either the mobile station or the base station. (Col. 7, lines 1-4 and lines 33-40). A secret key MBKEY is known by both the base station and mobile station and is used to authenticate each other. (See. Col. 7, lines 55-64). The base station (e.g., network element) receives a random number RDN_3 from the mobile station and generates a message signed with a digital signature. The signed message is then encrypted using the secret key MBKEY and sent to the mobile station. (Col. 8, lines 6-9).

U.S. Ser. No. 09/863,139
Attorney Docket No. 010055B1

Upon further review of the portions cited in the Office Action, there seems to be nothing in Juopperi to even suggest "generating a primary signature based upon a key that is held private from the mobile station and a secondary signature that is received from the mobile station as claimed" as claimed.

The Office Action states the secret key MBKEY in Juopperi is the "key held private from the mobile station." However, Juopperi clearly teaches that the secret key MBKEY is known to both the base station and the mobile station. (Col. 7, lines 55-61). In fact, it is the knowledge of this common secret key MBKEY that allows the mobile station to authenticate the base station in Juopperi. By contrast, in the present claimed invention the "key [is] held private from the mobile station."

Moreover, a primary signature is not generated based upon a key (MBKEY) as claimed. Juopperi teaches that the MBKEY is used to encrypt a message from the base station to the mobile station. It is not used to generate a composite primary signature as claimed.

Additionally, Juopperi also does not appear to teach "generating a primary signature based upon ... a secondary signature that is received from the mobile station" as claimed. In particular, while the base station receives a random number RDN_3 from the mobile station, it is not a signature that is used to generate the primary signature as claimed.

Since Juopperi does not teach at least the above elements of claim 17, Applicant submits that Juopperi does not teach all elements of claim 17 and therefore, claim 17 is allowable. Also, Applicant has also added new independent claims 30, 31, and 32 corresponding to independent claim 17. New claims 30, 31, and 32 have substantially the same scope as claim 17. Accordingly, Applicant submits that these claims are believed to be allowable as well.

U.S. Ser. No. 09/863,139
Attorney Docket No. 010055B1

For at least the foregoing reasons, Applicant respectfully submits that Juopperi does not teach every element of the claims and request a withdrawal of the rejection under 35 U.S.C. §102.

Applicant has reviewed the references made of record and asserts that the pending claims are patentable over the references made of record.

II. ALLOWED CLAIMS

Applicant notes with appreciation the Examiner's allowance of claims 1-16 and request that they be promptly issued

Applicant has added new independent claims 18, 19, and 20 corresponding to allowed independent claim 1. New claims 18, 19, and 20 have substantially the same scope as allowed claim 1 and incorporate the limitation "concatenate the initial value with a received signal ..." which was identified by the Examiner as being novel. Therefore, Applicant submits that claims 18, 19, and 20 are in condition of allowance.

Applicant has also added new independent claims 21, 23, and 25 corresponding to allowed independent claim 8. New claims 21, 23, and 25 have substantially the same scope as allowed claim 8 and incorporate the limitations "receiving a secret key from a key generation element and information from a mobile unit", "concatenating the secret key with the information from the mobile unit", and "hashing the concatenated secret key and information to generate a signature" which were identified by the Examiner as being novel. Therefore, Applicant submits that claims 21, 23, and 25 are in condition of allowance.

Applicant has also added new independent claims 27, 28, and 29 corresponding to allowed independent claim 11. New claims 27, 28, and 29 have substantially the same scope as allowed claim 11 and incorporate the limitations "generating a plurality of keys from a received

APR 17 2007

U.S. Ser. No. 09/863,139
Attorney Docket No. 010055B1

value and a secret value", "delivering at least one communication key from the plurality of keys to a communication unit configured to interact with the subscriber identification module", and "hashing a version of the at least one secret key together with an authorization message ...", which were identified by the Examiner as being novel. Therefore, Applicant submits that claims 27, 28, and 29 are in condition of allowance.

CONCLUSION

In light of the amendments contained herein, Applicant submits that the application is in condition for allowance, for which early action is requested.

Applicant requests a two month extension of time in which to respond to the Office Action dated November 17, 2006. Please charge the requisite extension fee to Deposit Account No. 17-0026. Please charge any other fees associated with this paper to deposit Account No. 17-0026.

Respectfully submitted,



Dated: April 17, 2007

By: /s/ David Huffaker
David J. Huffaker, Reg. No. 56,771
Attorney for Applicant
Telephone: 858-845-2110

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502